"Experiences from the incorporation of international rules and guidelines on the safety of nuclear power plants into the German nuclear rules and regulations"

Ch. Wassilew, R. Donderer, M. Mertins

Abstract

According to the German Atomic Energy Act, a licence for operating a nuclear power plant (NPP) may only be granted if it has been proven by the licensee that the necessary precautions as required by the state-of-the-art against damage that may occur as a result of the plant operation have been taken. In Germany, the safety related requirements governed by this mandatory precaution are laid down in a detailed set of nuclear regulations. Clearly defined review processes ensure that the nuclear regulations are continuously being compared to the developments of the state-of-the-art and are adapted to it, if necessary.

The state-of-the-art to be applied in the frame of reviewing the nuclear regulations is determined by:

- the results evaluating the operating experience world-wide,
- the results of nuclear safety research and safety assessment,
- lessons learnt from the licensing and supervision of nuclear power plants,
- the development of international safety standards for nuclear power plants.

International nuclear standards are in particular the Guides of the IAEA published in the IAEA SAFETY STANDARDS SERIES - REQUIREMENTS and the recommendations of the Western European Nuclear Regulators' Association (WENRA).
The defence-in-depth concept, embedded in a comprehensive Man-Technology-Organisation (MTO) structure, represents the central technical approach for the review and modernisation of nuclear regulations.

The work for enhancing the nuclear regulations has involved wide circles of experts as well as interested members of the general public, especially through the use of the possibilities offered by the Internet, and has taken approx. 5 years.

The paper outlines the process of reviewing the existing nuclear regulations and presents the main technical aspects of the actual enhanced safety related rules that will

replace the existing ones in the future. It also describes the work in connection with the integration of international safety standards for nuclear power plants as well as the corresponding assessment results.

Standardized and universally acceptable nuclear regulations and standards are a key issue to strong regulatory bodies and harmonized regulatory strategies.

Part I: Regulatory Aspects

1 Nuclear Energy in Germany

Currently, 17 nuclear power plant units are in operation at 12 different sites in Germany producing a total of 21,475 MW_e. Figure 1 gives a survey of the nuclear power plants in operation.

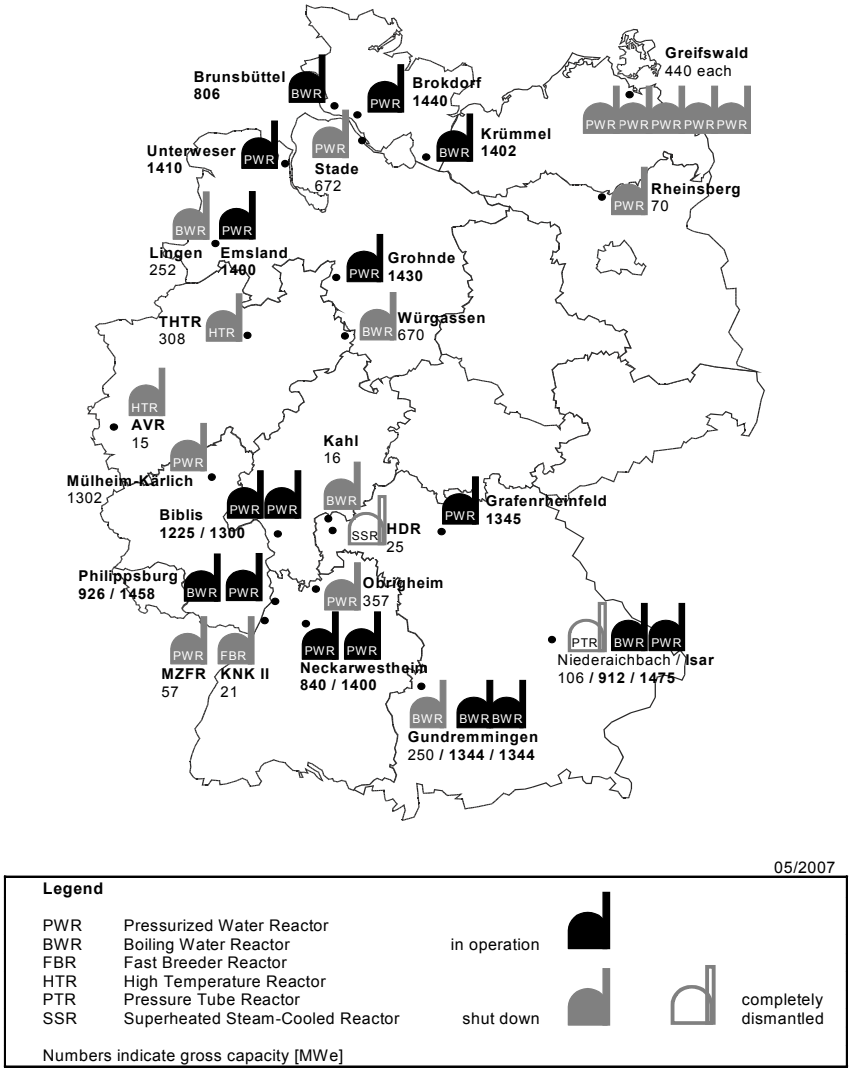

Fig. 1 Nuclear power plants in Germany

According to the design at the time of their construction, the nuclear power plants with pressurised water reactors can be classified according to four generations, whereas those with boiling water reactors belong to two different generations. The classification according to generations and construction lines is presented in Table 1.

Table 1 German nuclear power plants in operation

	NPPs in operation Site	a) Licensee b) Manufacturer c) Major shareholder	Type Gross-capacity MW_e	Constr. Line	a) Date of application b) First criticality
1	Biblis A (KWB A) Biblis Hessen	a) RWE Power b) KWU c) RWE Power 100 %	PWR 1225	2	a) 11.06.1969 b) 16.07.1974
2	Biblis B (KWB B) Biblis Hessen	a) RWE Power b) KWU b) RWE Power 100 %	PWR 1300	2	a) 03.05.1971 b) 25.03.1976
3	Neckarwestheim 1 (GKN 1) Neckarwestheim Baden-Württemberg	a) EnBW Kernkraft (EnKK) b) KWU c) EnKK 98.45 %	PWR 840	2	a) 02.04.1971 b) 26.05.1976
4	Brunsbüttel (KKB) Brunsbüttel Schleswig-Holstein	a) Kernkraftwerk Brunsbüttel b) AEG/KWU c) Vattenfall Europe Nuclear Energy 66.7 %	BWR 806	69	a) 10.11.1969 b) 23.06.1976
5	Isar 1 (KKI 1) Essenbach Bayern	a) E.ON Kernkraft b) KWU c) E.ON Kernkraft 100 %	BWR 912	69	a) 25.06.1971 b) 20.11.1977
6	Unterweser (KKU) Esenshamm Niedersachsen	a) E.ON Kernkraft b) KWU c) E.ON Kernkraft 100 %	PWR 1410	2	a) 07.04.1971 b) 16.09.1978

	NPPs in operation Site	a) Licensee b) Manufacturer c) Major shareholder	Type Gross-capacity MW_e	Constr. Line	a) Date of application b) First criticality
7	Philippsburg 1 (KKP 1) Philippsburg Baden-Württemberg	a) EnBW Kernkraft (EnKK) b) KWU c) EnKK 100 %	BWR 926	69	a) 20.02.1970 b) 09.03.1979
8	Grafenrheinfeld (KKG) Grafenrheinfeld Bayern	a) E.ON Kernkraft b) KWU c) E.ON Kernkraft 100 %	PWR 1345	3	a) 07.06.1973 b) 09.12.1981
9	Krümmel (KKK) Krümmel Schleswig-Holstein	a) Kernkraftwerk Krümmel b) KWU c) Vattenfall Europe Nuclear Energy 50 % E.ON Kernkraft 50 %	BWR 1402	69	a) 18.02.1972 b) 14.09.1983
10	Gundremmingen B (KRB B) Gundremmingen Bayern	a) Kernkraftwerk Gundremmingen b) KWU c) RWE Power 75 %	BWR 1344	72	a) 15.03.1974 b) 09.03.1984
11	Grohnde (KWG) Grohnde Niedersachsen	a) Gemeinschaftskernkraftwerk Grohnde b) KWU c) E.ON Kernkraft 83.3 %	PWR 1430	3	a) 03.12.1973 b) 01.09.1984
12	Gundremmingen C (KRB C) Gundremmingen Bayern	a) Kernkraftwerk Gundremmingen b) KWU c) RWE Power 75 %	BWR 1344	72	a) 15.03.1974 b) 26.10.1984

	NPPs in operation Site	a) Licensee b) Manufacturer c) Major shareholder	Type Gross-capacity MW_e	Constr. Line	a) Date of application b) First criticality
13	Philippsburg 2 (KKP 2) Philippsburg Baden-Württemberg	a) EnBW Kernkraft (EnKK) b) KWU c) EnKK %	PWR 1458	3	a) 24.06.1975 b) 13.12.1984
14	Brokdorf (KBR) Brokdorf Schleswig-Holstein	a) E.ON Kernkraft b) KWU c) E.ON Kernkraft 80 %	PWR 1440	3	a) 12.03.1974 b) 08.10.1986
15	Isar 2 (KKI 2) Essenbach Bayern	a) E.ON Kernkraft b) KWU c) E.ON Kernkraft 75 %	PWR 1475	4 Konvoi	a) 13.02.1979 b) 15.01.1988
16	Emsland (KKE) Lingen Niedersachsen	a) Kernkraftwerke Lippe-Ems b) KWU c) RWE Power 87.5 %	PWR 1400	4 Konvoi	a) 28.11.1980 b) 14.04.1988
17	Neckarwestheim 2 (GKN 2) Neckarwestheim Baden-Württemberg	a) EnBW Kernkraft (EnKK) b) KWU c) EnKK 98.45 %	PWR 1400	4 Konvoi	a) 27.11.1980 b) 29.12.1988

Since 1988, nuclear energy has been covering approx. one third of the public electricity supply and about 12 % of the entire primary power supply in Germany.

The Atomic Energy Act in its current version limits the remaining electricity output yet to be generated and thus the operating lives of the plants (Table 1). These licences for the nuclear power plants were granted after the applicant had proved to the nuclear licensing authority that the required protection against damage according to the state-of-the-art at the respective time was achieved by the plant design and construction and the on-site provisions applied for.

This licensing prerequisite applies both to the licences granted after that and the licences yet to be granted for major modifications of the plant itself or of its mode of operation. This way, each major modification performed within the framework of the object of the modification procedure, results in a safety review and, where required, in an adaptation to necessary precautions against damage according to the state-of-the-art.

Furthermore, the authority may revoke the licence, if this licensing prerequisite is no longer fulfilled or cannot be fulfilled within a reasonable time.

Over the past years, numerous improvements have been realized at all nuclear power plants in the course of their operating lives, in particular also by measures in the area of beyond-design basis accidents. Thus, safety precautions and risk prevention for the nuclear power plants have been further developed in accordance with the progress of the state-of-the-art.

The safety of the plant is continuously reviewed within the frame of regulatory supervision. In case of any new safety relevant findings, the need for improvements is determined. This also contributes to further developing plant safety.

Periodic Safety Reviews (PSRs) are performed to supplement the continuous regulatory supervision process. In 2002, they were made mandatory due to the Atomic Energy Act.

2 Licensing and Supervision

The Federal Republic of Germany is a federal state. Responsibilities for legislation and execution are assigned to the organs of the Federation and the so-called *Länder (federal states)* according to their scope of functions. Unless otherwise specified, the execution of federal law lies in principle within the sole responsibility of the federal states, the *Länder*. The "Regulatory Body" is therefore composed of federal government and *Länder* government authorities. The interaction between the Federation and the *Länder* in the field of nuclear safety is presented in Figure 2.

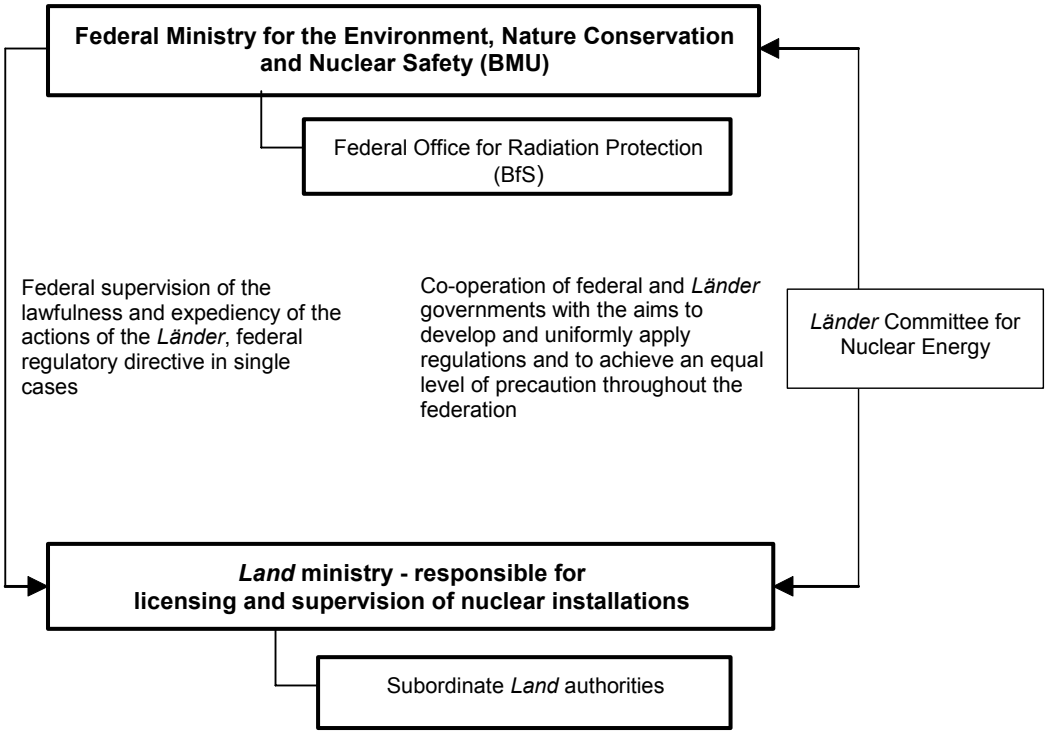

Fig. 2 Interaction between the Federation and the *Länder*

Specifications are given by provisions of the Basic Law (Constitution) of the Federal Republic of Germany.

The Federal Government has the legislative competence for the peaceful use of nuclear energy. According to Articles 87c and 85 of the Basic Law, the Atomic Energy Act is executed - with some exceptions - by the *Länder* on behalf of the Federal Government. That means that the *Länder* regulators are under the supervision of the Federation with regard to the lawfulness and appropriateness of their actions.

The Atomic Energy Act covers the general national regulations for protective and preventive measures, radiation protection, and disposal of radioactive waste and irradiated fuel elements in Germany and represents the basis for the associated statutory ordinances.

With respect to the protection against the hazards from radioactive materials and to the supervision of their utilisation, the Atomic Energy Act requires the construction and operation of nuclear installations to be subject to regulatory licensing. Prerequisites and

procedures for licensing and the performance of supervision are specified, including the regulations for the consulting of experts and charging of costs.

There are ordinances, among others, on radiation protection, the nuclear licensing procedures, protective and preventive measures at nuclear power plants, the nuclear safety officer and the reporting on special events, nuclear reliability assessment and nuclear financial security.

The more detailed guidelines, recommendations and safety standards of the Nuclear Safety Standards Commission (KTA) become binding by specification in the license or by supervisory measures in the individual case.

The licensing of nuclear installations is regulated in the Atomic Energy Act. According to Section 7 of this Act, a licence is required for the construction, operation, essential modifications of the plant or its operation and also for decommissioning. When issuing a licence, obligations may generally be imposed. Any act of operating, essentially modifying or decommissioning a nuclear installation without the required corresponding licence is punishable by law.

According to the applicable law, licences for the construction of nuclear power plants for the commercial production of electricity are no longer issued in Germany. The authorisation for power operation of the existing nuclear power plants expires once the amount of electricity for the respective plant as stipulated in the Atomic Energy Act or the electricity volume derived from transfers has been produced. Therefore, licensing procedures are only performed for the modification of existing nuclear installations and for decommissioning.

The planned modifications of a nuclear power plant or its operation are to be assessed systematically with regard to their impacts on the necessary protective and preventive measures and are to be treated accordingly in the procedure.

Modifications that may have greater than obviously insignificant impacts on the safety level of the nuclear installations are subject to licensing pursuant to Section 7 (1) of the Atomic Energy Act. In addition, there are modifications having only insignificant impacts on the safety level and therefore are not subject to licensing but require accompanying inspections by the safety authorities within the framework of the supervisory procedure.

For modifications requiring a licence, the fulfilment of the licensing prerequisites is to be verified according to Section 7 of the Atomic Energy Act.

The actual details and procedures of licensing in accordance with the Atomic Energy Act are specified in the Nuclear Licensing Procedure Ordinance. It deals specifically with the application procedure, with the submittal of supporting documents, with the participation of the general public and with the possibility to split the procedure into several licensing steps (partial licences). Furthermore, it deals, with the assessment of environmental impacts and the consideration of other licensing requirements (e.g. regarding the potential release or discharge of non-radioactive pollutants into air or water).

The Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) is the ministry responsible for nuclear safety and radiation protection. Hence the BMU is the supreme regulatory authority in charge of nuclear safety and security in Germany.

The fundamental regulations for the further official competences are contained in the Atomic Energy Act in Sections 22 - 24. According to Section 24, the respective *Länder* governments determine the supreme *Länder* authorities in charge of the licensing and supervision of nuclear power plants.

Licensing and supervisory authorities for nuclear installations are ministries of the *Land,* in which the nuclear installation is located. The BMU is the Federal German supervisory authority.

In accordance with Section 20 of the Atomic Energy Act, the competent authorities may involve authorised experts in technical or scientific questions related to regulatory licensing and supervision having, similar to the authorities, the right of inspections and requesting information. By involving authorised experts, an evaluation of the safety issues is performed being independent of that of the licence applicant. The authorised experts perform their own tests and evaluations and their own calculations, preferably with methods and computer codes different from those used by the licence applicant. The persons involved in preparing the expert opinions are not bound by any technical directives. In making their decisions, the authorities are not bound by the authorised experts' evaluation results. For the Federal supervisory activities, the BMU will equally consult national and international experts if necessary.

The interaction of the different authorities and organisations involved in the nuclear licensing procedure and the participation of the general public is shown in Figure 3.

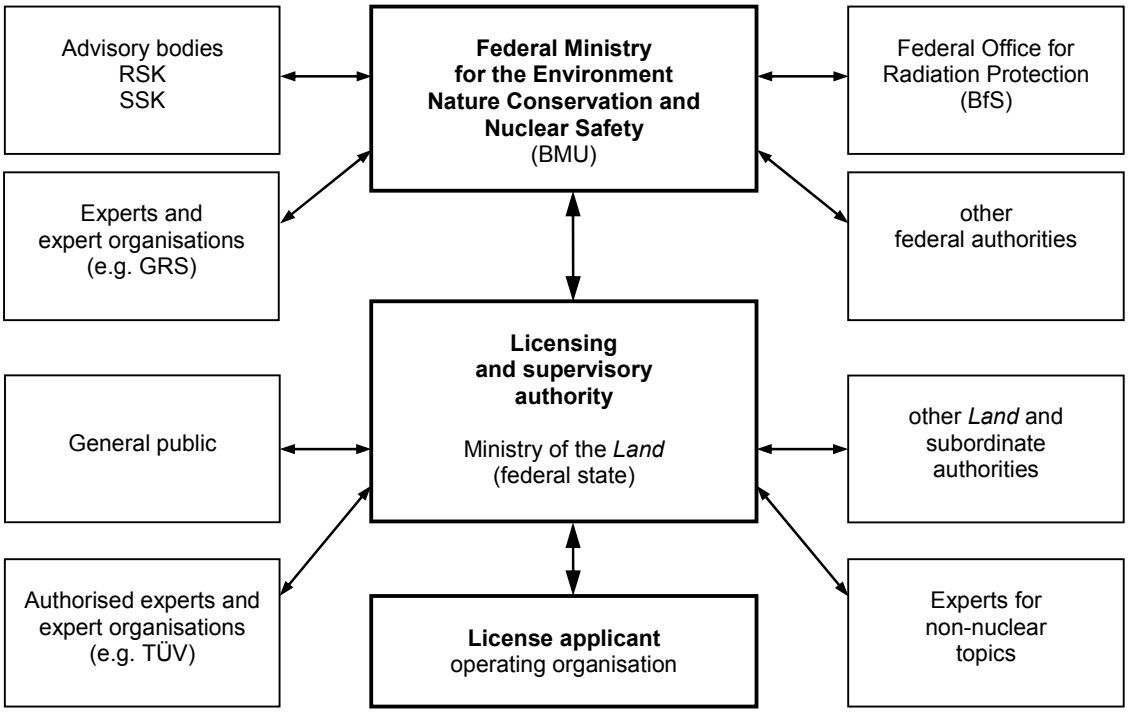

Fig. 3 Participants in the nuclear licensing procedure

3 Survey of nuclear regulations in Germany

Figure 4 presents the hierarchy of the national rules and regulations, the authority or institution issuing the regulation and their degree of bindingness.

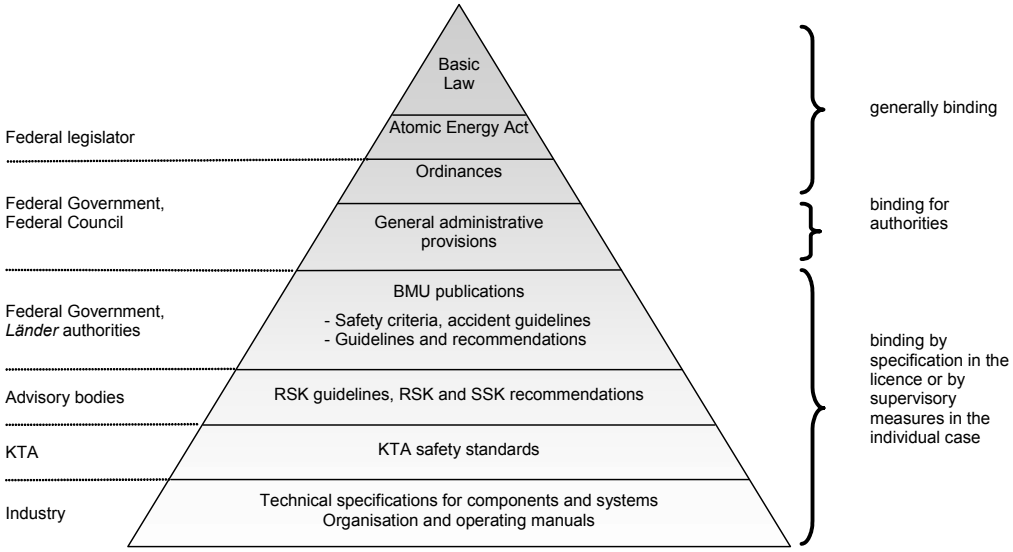

Fig. 4 Regulatory pyramid

Nuclear regulations, except laws, ordinances and general administrative provisions, only have regulatory relevance due to the legal requirement regarding the state-of-the-art. The dynamic improvement of the safety requirements requested by law is not bound to the formal development of standards.

The updating processes of nuclear laws, the associated provisions and the general administrative provisions lie within the responsibilities of the regulatory body. The non-mandatory guidance instruments, as the Safety Criteria or the accident guidelines, largely date back to the seventies and the eighties of the 20th century. Since then, the practices of licensing and regulatory enforcement, the rules and regulations of the KTA safety standards and also those established by international organisations and in other countries have continuously been further developed.

Therefore, the BMU initiated a project at the end of 2003 on the development of an integrative and consistent set of rules and regulations for assessing the safety of German nuclear power plants.

This framework shall include the fundamental safety requirements among others of the existing safety criteria of the Federal Ministry of the Interior (BMI) and of the existing guidelines of the Reactor Safety Commission, shall describe the state-of-the-art and, among others, consider the international regulations as well as practical experience from the application of the existing German nuclear rules and regulations. Draft versions of the new integrative and consistent set of rules and regulations were discussed with the stakeholders within the framework of workshops and by using the Internet. A new draft of the “Safety Criteria for Nuclear Power Plants” (Revision C) was submitted in September 2008, the last version of the “Safety Criteria for Nuclear Power Plants” is available since April 2009.

Part II: Technical Aspects

4 Update of the Nuclear Rules and Regulations

A focal point of the work on the update of the nuclear rules and regulations was the determination of the state-of-the-art in the field of nuclear safety. For this purpose, in addition to the applicable rules and regulations, the experiences from the operation of nuclear power plants were referred to, results from safety reviews and analyses as well as from scientific studies were evaluated and the findings from the comparison with international nuclear rules and regulations were included.

The BMU project concerning the update of the nuclear rules and regulations was performed to update the existing regulations in accordance with the current state-of-the-art to achieve a comprehensive and systematic framework. The Safety Criteria for Nuclear Power Plants describe the design and the operation of nuclear power plants according to the most advanced state in Germany, taking into account the international state-of-the-art in. The Safety Criteria for Nuclear Power Plants consider, among other aspects, the latest versions of the rules of the IAEA (NS-R-1, NS-R-2, NS-R-3, GS-R-3) as well as the reference levels defined by WENRA within the framework of a comparison of international best practices.

The BMU has set basic principles for drafting of the “Safety Requirements for Nuclear Power Plants”:

- Consistent implementation of the integrative Man-Technology-Organisation (MTO) concept;
- Consistent allocation of the safety requirements to the levels of defence of the “defence-in-depth concept“ and to the “barrier concept“;
- Consideration of all conditions of power operation and low-power and shutdown states;
- Consistent deterministically oriented safety concept.

Considering these basic principles, the team in charge has been developing 12 new rules for all relevant safety aspects. New rules are structured by topics:

- Module 1: Fundamental Safety Requirements
- Module 2: Requirements for the Design of the Reactor Core
- Module 3: Events to be Considered for PWRs und BWRs
- Module 4: Requirements for the Design of the Reactor Coolant Pressure Boundary, the Pressure-Retaining Walls of the External Systems and the Containment System
- Module 5: Requirements for I&C
- Module 6: Requirements for Safety Demonstration
- Module 7: Requirements for Accident Management
- Module 8: Requirements for Safety Management
- Module 9: Requirements for Radiation Protection
- Module 10: Requirements for the Design and Safe Operation of Plant Structures, Systems and Components
- Module 11: Requirements for the Handling and Storage of the Fuel Elements
- Module 12: Requirements for Emergency Power Supply

The updated nuclear rules comprise requirements on all areas that are essential for the safety of nuclear power plants.

Compared to the existing regulations the new rules comprise additions to provide for

- Consistent introduction of the 4th level of defence, in particular introduction of Severe Accident Management Guidelines (SAMGs)
- Requirements for safety management systems (SMS)
- Greater stress on requirements for safe operation
- Additions regarding instrumentation and control (I&C)
  - Requirements for software-based I&C

- Full inclusion of requirements for BWR type reactors

- Additions regarding demonstration methods

To the additions in detail:

- Consistent introduction of the 4th level of defence, in particular introduction of Severe Accident Management Guidelines (SAMGs)

The aim of the fourth level of defence is to ensure that radioactive releases caused by severe accidents are kept as low as practicable.

Level 4 of the defence-in-depth concept is achieved by providing equipment and procedures to manage accidents and mitigate their consequences as far as practicable.

Most importantly, adequate protection is provided for the confinement function by way of a robust containment design. This includes the use of complementary design features to prevent accident progression and to mitigate the consequences of selected severe accidents. The confinement function is further protected by severe accident management procedures.

In the new rules credible BDBAs are identified, based on operational experience, engineering judgment, and the results of analysis and research. This includes events leading to significant core degradation (severe accidents), particularly those ones challenging the containment. It is required that the safety concept of the nuclear power station should be balanced such that no particular design feature or event makes a dominant contribution to the frequency of severe accidents, taking uncertainties into account.

By the new rules complementary equipment and procedures are required with the goal of preventing identified BDBA scenarios, and mitigating their consequences if they do occur.

The new rules that have been applied to the complementary equipment and procedures do not necessarily need to incorporate the same degree of conservatism as those applied to the design basis.

In the case of multi-unit plants, the use of available support from other units is relied upon only, if it can be established that the safe operation of the other units is not compromised.

On the basis of the credible BDBAs identified, the equipment and procedures to be used in the management of severe accidents have to be defined. Particular attention is paid to the prevention of potential containment bypass in accidents involving significant core degradation.

Consideration is given to the plant's full design capabilities, including the possible use of safety, non-safety, and/or temporary systems, beyond their originally intended function. This applies to any system that can be shown with a reasonable degree of assurance to be able to fulfill their required function in the environmental conditions expected during a severe accident.

The containment maintains its role as a leak-tight barrier for a period that allows sufficient time for the implementation of off-site emergency procedures following the onset of core damage. The containment also prevents uncontrolled releases of radioactivity after this period.

The new rules furthermore require the establishing Severe Accident Management Guidelines (SAMGs). The SAMGs are used in the case of a loss of function of the equipment installed.

With the implementation of the fourth level of defence in the safety concept of operating NPPs, events are taken into account in the defence-in-depth concept, which originally have not been considered as design basis accidents due to their low probability of occurrence. At this level, measures are provided against specific, very rare events such as aircraft crashes, external blast waves and anticipated transients without scram (ATWS). To cope with these events, there are reduced requirements in comparison with the third level of defence, but the verification is similar. Moreover, accident management measures have been implemented at this level since the eighties in order to detect beyond-design basis accidents timely and reliably, to keep them under control and to bring them to an end with as little damage as possible.

The preventive measures of accident management are to avoid serious core damage. The main goal is to maintain or restore cooling of the reactor core and to convey the

nuclear power plant into a safe condition. On the other hand, the mitigating measures are foreseen to reduce serious radiological impact on the plant site and the environment. Here, the main goal is to maintain the activity retaining barriers being available and to ensure long-term controlled conditions of the plant for the protection of the environment.

This defence-in-depth concept with its four levels of safety has meanwhile been implemented in all German nuclear power plants.

The accident management measures are based on a flexible utilization of available safety and operating systems even beyond design usage – even at the risk of them being damaged – and on the utilization of external systems. Extensive technical and administrative precautions have been taken in the German nuclear power plants in order to be able to perform effective accident management measures in case an event would actually occur.

In addition to the introduction of emergency operating procedures in all plants, the precautions in the case of **pressurized water reactors** to ensure core cooling concern the **preventive measures**:

- secondary side feed and bleed,
- primary side feed and blfeed,

and for activity retention the **mitigation measures**:

- assured containment isolation,
- RPV primary side bleed,
- hydrogen countermeasures,
- supply-air filtering for the main control room.

In the case of **boiling water reactors** the **preventive measures** to ensure core cooling concern:

- an independent injection system,
- the additional possibility of injection into and refilling of the reactor pressure vessel,

and the **mitigatingon measures** for activity retention:

- assured containment isolation,
- pressure relief of the reactor pressure vessel,
- filtered containment venting,
- inertisation of the containment atmosphere (reactors of the construction line 69) or of the pressure suppression pool air volume only, supplemented by H_2-countermeasures (construction line 72 reactors), and
- supply-air filtering for the main control room.

Auxiliary measures supporting the preventive and mitigation measures in both reactor types are:

- Sufficient capacity of the batteries or emergency power supply from neighbouring plant units (if existent),
- possibilities for a fast restoration of off-site power supply,
- an additional off-site power supply (underground cable),
- sampling system in the containment,
- emergency organisation with training and emergency exercises.

The functional efficiency of the accident management measures should be demonstrated on the basis of representative estimates and plausibility considerations. The accident management measures have generally to be feasible, appropriate and effective, as well as compliant with the safety concept of the respective plant. The fulfilment of these requirements has to be verified in the corresponding licensing and supervisory procedures.

- Requirements for safety management systems (SMS)

By the new rules the operators are called upon to develop management systems and install and operate them in their plants. The aim of such management systems is to commit them to a high level of safety and to enhance safety culture. It is to ensure that safety is given priority over other business objectives.

The Guideline for Safety Management was already published by the BMU in 2004. The operators in Germany assured that SMS was fully implemented and reported it to the BMU in August 2008. Operators have to apply a SMS in the day-to-day operation and improve it continuously.

The aims of the SMS are high safety culture, foresighted planning, acting in the interest of safety, and fortification of the licensee‘s initiative for continuous improvement.

- Greater stress on requirements for safe operation

In the new rules the plant states are grouped into the following four categories (Figure 5):

Normal Operation - operation within specified OLCs, including start-up, power operation, shutting down, shutdown, maintenance, testing, and refuelling;

Anticipated Operational Occurrence - a deviation from normal operation that is expected to occur once or several times during the operating lifetime of the NPP but which, in view of the appropriate design provisions, does not cause any significant damage to any items important to safety, nor lead to accident conditions;

Design Basis Accidents - accident conditions for which an NPP is designed according to established design criteria, and for which damage to the fuel and the release of radioactive material are kept within regulated limits; and

Beyond Design Basis Accidents - accident conditions less frequent and more severe than a design basis accident. A BDBA may or may not involve core degradation.

Acceptance criteria are assigned to each plant state, taking into account the expectation that frequent PIEs will have only minor or no radiological consequences, and events that may result in severe consequences are of extremely low probability.

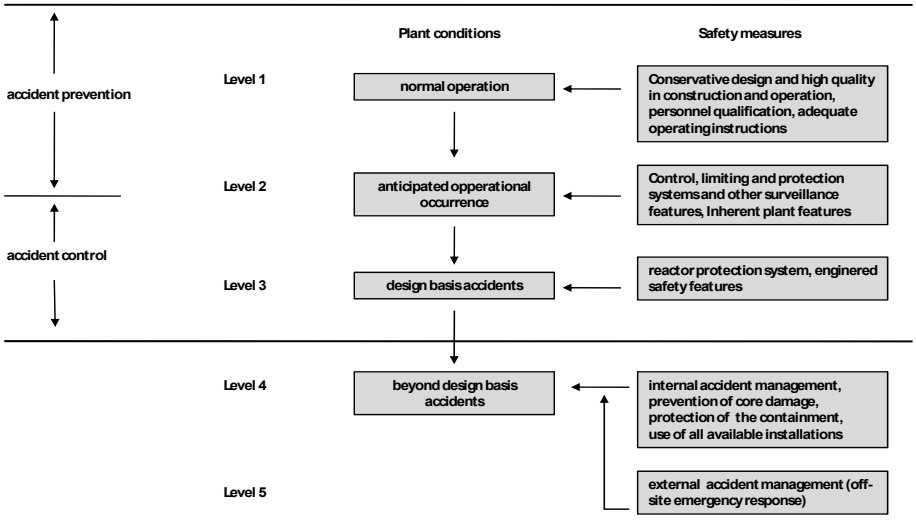

Fig. 5 Plant states of the NPP

The new rules require among other things that the unavailability of safety systems has to be minimized. The NPP addresses the potential for accidents that might occur if the availability of safety systems is reduced, such as during shutdown, start-up, low power operation, refuelling, and maintenance. The operator has to ensure that the requirements are met and that due account is taken of the human capabilities and limitations of personnel. Furthermore the operator has to ensure safe operation and maintenance of the plant including subsequent plant modifications, and has to provide

practices for incorporating the safety information into the plant administrative and operational procedures (i.e. operational limits and conditions).

According to the Nuclear Licensing Procedure Ordinance in Germany a compilation has to be submitted as part of the application documents containing all the data relevant to the safety of the plant and its operation, the measures to be taken in the event of any incidents or damage, and an outline plan of the in-service inspection tests provided for safety-related components of the plant.

The safety specifications constitute a binding and updated documentation of the licensed and, in terms of safety, reliable frame for the condition and mode of operation of the plant (operational limits and conditions for safe operation). They are the basis upon which the safety relevance of modifications of the plant or its operation will be assessed. As a matter of principle, modifications concerning data contained in the safety specifications require the approval of the licensing or supervisory authority in charge.

For the design of the plant, the design principles laid down in the nuclear rules and regulations are to be applied and the ability to control design basis accidents has to be verified.

On this basis, limits and conditions for operation and measures for the control of accidents are derived. These are documented as the so-called safety specifications in accordance with the Nuclear Licensing Procedure Ordinance and with the Guidelines Concerning the Requirements for Safety Specifications for Nuclear Power Plants. They give a quick and comprehensive survey of all data, limits, conditions, requirements and measures that determine the safety of the nuclear installation. The safety specifications are a constituent part of the operating manual and the testing manual.

The operating manual is the most important working document for the plant personnel. It contains all operating and safety-related instructions required for normal operation of the plant as specified and for the control of incidents as well as plant regulations applicable for all persons working at the plant. Structure and contents of the operating manual are described in the nuclear rules and regulations in KTA Safety Standard. The safety specifications are included in the operating manual as a separate chapter or as marked sections. Any modifications of the safety specifications require approval by the

licensing or supervisory authority. The limits and conditions of safety operation in the safety specifications prescribed by the licensing authority must be met at all times.

The organisational procedures required for a safe and licence-conform operation of the plant are laid down in the operating manual and the testing manual.

All nuclear power plants have an operating manual. Structure and contents of the operating manual of a nuclear power plant are laid down in a KTA Safety Standard. The operating manual covers the plant regulations valid throughout the plant, as well as instructions for operating and accident conditions, such as detailed instructions for the shift personnel with additional information regarding the particular plant conditions involved. All parts of the operating manual that belong to the safety specifications are marked accordingly.

The **operating manual** consists of the following parts:

- *Plant regulations*

These comprise the personnel organisation (tasks, responsibilities, subordination, etc.), control room and shift regulation, maintenance regulation, radiation protection regulation, guard and access regulation, alarm regulation, fire protection regulation and first aid regulation. All plant regulations are part of the safety specifications.

- *Plant operation*

This part contains the prerequisites and conditions for operation and the safety system settings, the criteria for the reporting of events to the supervisory authority and detailed instructions for normal and abnormal operation of the plant.

- *Design basis accidents*

This part of the operating manual includes the design basis accidents with and without loss-of-coolant and accidents originating from external impacts and the related procedures to control these accidents.

- *Systems operation*

This part covers the initial conditions for the different operating modes for all systems and the actions to be taken by the shift personnel as step programmes. In addition, it contains supplemental information, technical drawings and remarks.

- *Alarms*

This is a complete listing by systems of all alarm signals from failures or dangerous conditions together with corresponding instructions on counteractions and possible alternatives.

Alarm plans and organisational structures for the control of possible emergencies are also specified in the operating manual.

The operating manual is kept up to date through a revision service. The copy of the operating manual in the plant control room also contains all modifications in process. All modifications of the operating manual are subject to the regulatory supervision.

Fulfilment of the regulations of the operating manual is checked by the regulator and through on-site inspections performed by its authorised experts. The control of organisational processes includes, e.g., keeping a shift log, performance of prescribed walkabouts, the proceeding for the change of shift or the handling of alarms and work authorisations. In the area of radiation protection, e.g., compliance with dose limits and regulations on controlled areas and on the storage of radioactive material are inspected. Apart from that, safety-relevant measured values for plant operation or emission of radioactive material are checked within the framework of on-site inspections.

The **testing manual** regulates the number and proceeding of the in-service inspections on safety-relevant plant systems and components to be performed by the plant operator.

The structure and contents of the testing manual are laid down in a KTA Safety Standard. The testing manual comprises general instructions, the testing schedule and corresponding testing instructions for all in-service inspections.

The general instructions deal with the application and handling of the testing manual and the corresponding preconditions, e.g. the administrative procedures regarding test performance and result evaluation, permissible deviation from test intervals, participation of authorised experts in the test performance and in the case of modifications of the testing manual.

The testing schedule contains a list of all in-service inspections important to safety. It covers the test object, extent of test, test interval, required plant conditions under which the test is performed and a clear notation of the testing instruction. The testing schedule is part of the safety specifications.

The testing instructions identify the test object and the reason for performing the test (e.g. licensing requirements), the testing method, the target and the extent of the test. It also lists the supporting measures and documents, and describes the prerequisites, the performance (in case of functional tests e.g. switching sequence programme) and documentation of the test as well as the procedure for establishing a defined final condition after the test. In addition to a correct testing procedure, the testing instructions ensure that the limits of safe operation are also not exceeded during tests.

At specified intervals, also defined in the testing schedule, the authorised experts participate in the in-service inspections carried out by the plant operator on behalf of the supervisory authority. The frequency of such participation depends on the safety significance of the respective inspection. The supervisory authority is informed about the results of the in-service inspections.

Modifications of the testing schedule or the testing instruction are reviewed by the supervisory authority by consultation of authorised experts.

Further, the procedure for maintenance or modifications is specified.

Although **abnormal occurrences during specified normal operation** will cause operational restrictions (e.g. reduction of reactor power in case of a failure of one reactor coolant pump) there will be no safety reasons to discontinue operation. In the

case of accidents, on the other hand, plant operation may be discontinued for safety reasons. Detailed procedural instructions are specified for the shift personnel covering the individual operating modes for each of the abnormal occurrences or design basis accidents dealt with in the licensing procedure. These are contained in Part 2 and 3 of the operating manual.

The procedures for the the control of **design basis accidents** are a combination of instructions based on protection goal oriented and event based approaches.

The procedures for the control of design basis accidents are based on the following types of written instructions and aids:

- accident sequence diagram,
- check of the fundamental safety functions criteria,
- accident decision tree,
- fundamental-safety-functions-oriented handling of accidents,
- event-oriented handling of accidents.

In case of an event leading to a reactor scram, an accident sequence diagram is available which specifies the proceeding of the shift personnel. In a first step, the shift personnel should control the fundamental safety function criteria to determine whether or not

- control of reactivity (subcriticality),
- cooling of fuel elements (coolant inventory, heat transport and heat sink), and
- confinement of radioactive material (in particular, integrity of the containment)

have been achieved, and thus the release of activity into the environment does not exceed the accident planning values. In case, a violation of one of the fundamental

safety functions criteria is detected, the respective procedures, oriented on the fundamental safety functions, are used to bring the plant parameters back into their normal range. If no violation of fundamental safety function criteria is detected and the event may be assigned to a known type of accident, the further proceeding will be based on event-oriented procedures. If beyond-design basis plant conditions are detected, the shift personnel will also consult the decision trees for severe accidents and will employ the accident management measures.

The transition from design basis accident procedures to accident management measures is described in the section “protection goal oriented procedure” of the operating manual.

For **beyond design basis events** the technical measures to be taken at the plant, the accident management measures and auxiliary means required are contained in a separate document, the **accident management manual**.

Part of the organisational prerequisites established in all nuclear power plants to control emergencies is an emergency response team that is supported by personnel from the operating staff. The emergency response team should be able to take up work within an hour. Suitable rooms, working appliances and means of communication are provided. Alarm procedures and organisational structures are specified in the operating manual, further technical measures and accident management procedures in the accident management manual.

- Additions regarding instrumentation and control (I&C), requirements for software-based I&C

In the new rules appropriate standards and codes for the development, testing, and maintenance of computer hardware and software are required for the design of systems or equipment important to safety that are controlled by computers. A top-down software development process is used to facilitate verification and validation activities. This approach includes verification at each step of the development process to demonstrate that the respective product is correct, and validation to demonstrate that the resulting computer-based system or equipment meets its functional and performance requirements.

If software provided by a third party vendor is used in systems or equipment important to safety, then the software - and any subsequent release of the software – has to be developed, inspected, and tested in accordance with standards of a category commensurate with the safety function provided by the given system or equipment.

The software development process, including control, testing, and commissioning of design changes, as well as the results of independent assessment of that process, must be reviewable and systematically documented in the design documentation.

Where a function important to safety is computer-based, it is required that the design incorporates fail-safe and fault tolerance features, and the additional complexity ensuring from these features results in an overall gain in safety;

The design shall have protection against physical attack, intentional and non-intentional intrusion, fraud, viruses, and other malicious threats; and the design allows an effective detection, location, and diagnosis of failures in order to facilitate timely repair or replacement of equipment or software.

To reduce the potential for common cause failures, diversity should be incorporated into the computer system architecture to the extent necessary to meet the safety and reliability requirements for the overall computer system. The choice of diversity type has to be justified.

At present, software-based I&C are used at German nuclear power plants for functions that are not assigned to the highest safety relevance (i.e. without direct significance for reliable design basis accident control but for accident prevention). These functions are provided, e.g., in the reactor control and limitation system as well as for I&C in auxiliary emergency systems.

Corresponding backfitting measures using digital I&C in the area of reactor and turbine control were performed, e.g., at the German plants Biblis A, Isar 2, Isar 1, Grohnde, Philippsburg 2, Krümmel and Emsland.

A reactor protection system with completely computer-based I&C was installed for the first time at the FRM II research reactor commissioned in 2004. Such a backfit is planned for the power reactors Neckarwestheim 1 and Biblis B.

- Full inclusion of requirements for BWRs

In general, the requirements of the current regulations in Germany are related to the PWRs. Up to now these requirements have been applied to BWR correspondingly.

In the new rules the safety related requirements for BWRs are integrated completely.

- Additions regarding demonstration methods

In the new rules, requirements are integrated as follows:

  - Deterministic event sequence analyses generally have to include a quantification of the uncertainties.

  - Probabilistic analyses are to be applied to supplement the deterministic safety verification.

  - Engineering methods may be used for safety verification under specified conditions.

In particular, the purpose of the probabilistic safety assessment is to:

  - identify accident scenarios with the potential for significant core degradation;

  - demonstrate that a balanced design has been achieved such that no particular design feature or event makes a dominant contribution to the frequency of severe accidents, taking uncertainties into account;

  - provide probability assessments for the occurrence of core damage states and major off-site releases;

  - identify systems for which design improvements or modifications to operating procedures could reduce the probability of severe accidents or mitigate their consequences; and

- assess the adequacy of plant accident management and emergency procedures.

In Germany, the PSA is conducted in accordance with the requirements specified in a regulatory guideline, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*.

The methods and data applied for the probabilistic safety analysis are described and published in supplementary technical documents ("PSA Methods" and "PSA Data") to the regulatory guidelines.

In the years 1990 to 2000, the operators of the German nuclear power plants performed probabilistic safety analyses for all German nuclear power plants as part of the Periodic Safety Review. Level 1 probabilistic safety analyses according to the regulatory guidelines do exist for all German nuclear power plants. They have resulted in technical and procedural improvements at the plants.

Common cause failures (CCF) are of particular significance for the PSA results. Thus, an important aspect of the improvements from the methodical point of view is the enhancement of the modelling and quantification of CCFs. A measure that may be taken to counteract CCFs is the additional introduction of diversities.

Corresponding measures for plant improvements as derived from the Level 1 internal events PSAfor full power operational states at the Philippsburg 1 NPP are provided in the following:

- Replacement of older level transmitters and selection of the combinations for minimisation of CCF by diversity and monitoring of the level transmitters, and

- Actuation of the low pressure injection system by the core temperature as diverse criterion to the filling level.

Results from low power and shutdown PSAs mainly lead to modifications in the area of administrative specifications.

The removal of deficiencies and improvement of the balance of the precautionary measures led to an increase in safety, which is also reflected in the PSA results.

During the updating process the BMU initiated a comprehensive discussion and participation process of the “Safety Criteria for Nuclear Power Plants“ with the involvement of:

- the Reactor Safety Commission (RSK) and the Commission of Radiological Protection (SSK),
- the supervisory and licensing authorities of the *Länder*,
- the technical inspection organisations (TÜVs),
- vendors and operators of nuclear power plants.

The communication process is presented in Figure 2:

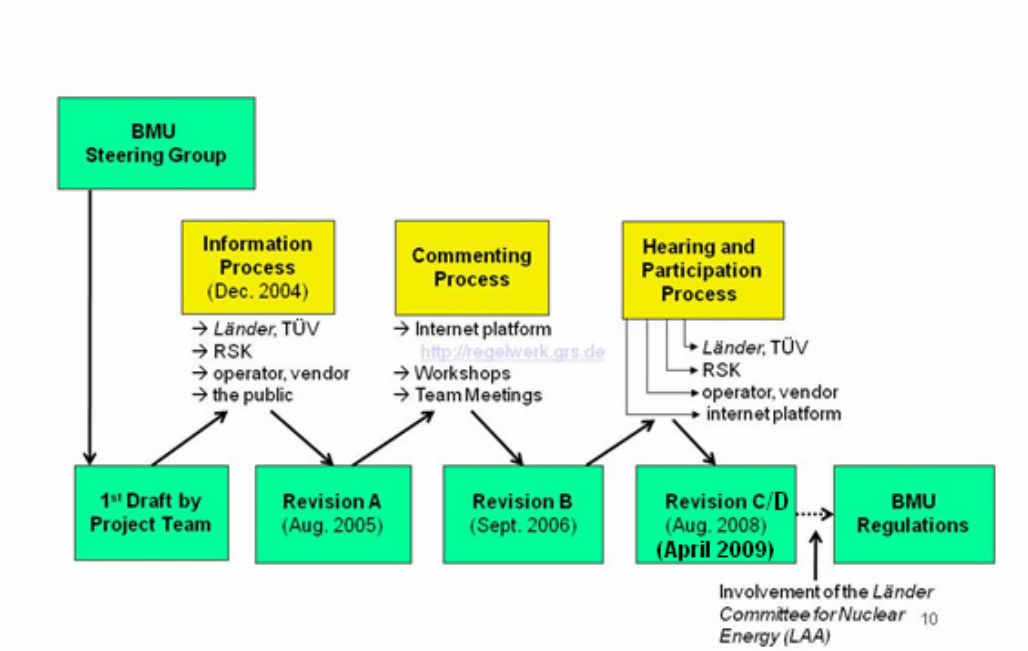

Fig. 2 Commenting process

Since the “Safety Criteria for Nuclear Power Plants“ were published on an Internet site, about 8,500 comments have been sent and taken into account during the revision process.

Focal points of the comments are, among others,

- Application of the safety requirements to older nuclear power plants:

By the new rules the existing safety criteria and guidelines have been revised. The new requirements are in compliance with the state-of-the-art in science and technology, as reflected by national and international practice and experience. The BMU has issued a position paper outlining a three-step implementation plan to advise the Länder Regulators on the use of the proposed document in relation to a safety assessment of existing facilities.

- The role of the PSA in safety assessments:

As for the PSA methods, the PSA manual is already provided with the consensus of PSA experts in Germany under the BMU PSA Guideline. The manual is very comprehensive and includes methods for:

- Level 1 PSA for internal and external hazards (e.g. plant internal fire, aircraft crash, gas explosion, flooding, seismic) for full power operational states,
- Level 1 PSA for low power and shutdown (LPS) states,
- Level 2 PSA for full power operational states,
- treatment of uncertainties and
- assessment of results.

The BMU is expected to provide guidelines on how to utilize PSA results in the regulation in Germany. Up to now no quantitative probabilistic criteria exist in Germany.

- Requirements for the beyond design basis area:

This defence-in-depth concept with its four levels of safety has meanwhile been implemented in all German nuclear power plants.

The accident management measures are based on a flexible utilisation of available safety and operating systems even beyond design usage – even at the risk of them being damaged – and on the utilisation of external systems. There are reduced requirements in comparison with the third level of defence. The functional efficiency of the accident management measures should be demonstrated on the basis of representative estimations and plausibility considerations. The accident management measures generally have to be feasible, appropriate and effective, as well as compliant with the safety concept of the respective plant.

- Requirements for digital I&C:

At present, software-based I&C are used in German nuclear power plants for functions that are not assigned to the highest safety relevance. These functions are provided, e.g., in the reactor control and limitation system as well as for I&C in auxiliary emergency systems. A reactor protection system with completely computer-based I&C was installed for the first time at the FRM II research reactor commissioned in 2004. Such a backfit is planned for the power reactors Neckarwestheim 1 and Biblis B.

To reduce the potential for common cause failures, diversity should be incorporated into the computer system architecture to the extent necessary to achieve the safety and reliability requirements for the overall computer system. The choice of diversity type has to be justified. The requirements in the new rules are based on deterministic principles.

Another focal point of the comments concerns the technical realisation of the “defence-in-depth concept“, in particular with regard to the independence of the individual levels of defence.

5 Summary and Conclusions

The safety standard in German safety practice is oriented on the applicable state-of-the-art. Safety and risk prevention at the nuclear power plants has been further developed accordingly.

The updating processes of nuclear laws, the associated provisions and the general administrative provisions lies within the responsibility of the regulatory body. The non-mandatory guidance instruments, as the Safety Criteria or the accident guidelines, largely date back to the seventies and the eighties of the 20th century. Since then, the practices of licensing and regulatory enforcement, the rules and regulations of the KTA Safety Standards and those established by the international organisations and in other countries have continuously been enhanced. At the end of 2003, the BMU initiated a project on the development of an integrative and consistent set of rules and regulations for assessing the safety of German nuclear power plants to reach compliance with the state-of-the-art also in this field. The last version of the newly developed nuclear rules and regulations has been available since April 2009 as “Safety Criteria for Nuclear Power Plants”.

A Nuclear Installations Safety Ordinance (AtASiV) is in preparation to be added to the existing statutory ordinances.

During the development of the "Safety Criteria for Nuclear Power Plants", all relevant safety standards of the International Atomic Energy Agency (IAEA) and the WENRA reference levels have been taken into consideration.

The current IAEA requirements and Guides as well as the WENRA reference levels have been assessed according to safety significant priorities, systematically compared with the current German nuclear rules and regulations, and commented on. Where appropriate, recommendations have been given for the update of the German rules and regulations.

The "Safety Criteria for Nuclear Power Plants" are based on the current nuclear rules and regulations in Germany and are in compliance with the international recommendations of the IAEA and WENRA.